REMARKS:

Claims 1-5, 28, and 29 stand rejected under 35 U.S.C. 102(b) as being anticipated by or under 35 U.S.C. 103(a) as being obvious over, the article "White Pine Upgrades Terminal Line" ("Anbinder"). In response, Applicant respectfully contends that these claims, as hereby amended, are patentable over Anbinder for the following reasons.

Amended claim 1 recites a device for use in a communication system including a transmitter, a receiver, and a serial communication link between the transmitter and the receiver. The system is configured to implement a content protection protocol which requires that each of the transmitter and the receiver has a distinctive value allocated thereto and must receive the distinctive value allocated to the other of the transmitter and the receiver during an authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the transmitter sends encrypted data to the receiver. The device includes circuitry coupled and configured to compare, during the authentication procedure, the distinctive values allocated to the transmitter and the receiver, and to prevent authentication from succeeding if the distinctive values are equal.

Anbinder discloses software that runs on terminals connected by a network. Anbinder teaches that when one terminal (to be called "Terminal A" for convenience) launches the software, the software checks for "serial number duplicates on the network." Apparently, each copy of the relevant software that can run on a terminal has a serial number associated with it. To check for software duplicates, the software running on Terminal A apparently receives the serial number associated with each copy of the software running on a terminal connected to the network. Anbinder teaches that if the software "detects another copy with the same serial number, the application tells you [emphasis added] who's running it so you [emphasis added] can correct the problem." Apparently, this is merely a suggestion by Anbinder that if another terminal ("Terminal B") is running a copy of software having the same serial number as the copy running on Terminal A, the software running on Terminal A informs the owner of the copyright in the software (or some other entity, identified as "you," but otherwise unspecified by Anbinder) that Terminal B is running a duplicate copy of the software.

Applicant specifically disagrees with the assertion in the Office Action that Anbinder teaches that a terminal running a copy of software "would only allow" another copy of the software running on another terminal "to run" if the serial numbers of the copies do not match. Applicant is unable to identify any teaching or suggestion in Anbinder that a terminal running a copy of software can or should (under any circumstance) prevent another copy of the software running on another terminal from running, and requests that the Examiner identify such teaching or suggestion if the assertion is maintained.

Anbinder fails to teach or suggest:

that any two of the terminals mentioned therein are coupled to each other by a serial communication link when implementing a content protection protocol, as are the transmitter and receiver recited in claim 1; or

that any two of the terminals mentioned therein are configured to implement a content protection protocol of the type recited in amended claim 1 (in which a transmitter and a receiver must successfully complete an authentication procedure before the transmitter sends encrypted data to the receiver); or

that any of the terminals mentioned therein is configured to perform an authentication procedure (a procedure performed by a transmitter and a receiver by which the transmitter verifies that the receiver is authorized to receive protected content from the transmitter or the receiver verifies that the transmitter is authorized to send protected content to the receiver) in accordance with a content protection protocol of the type recited in amended claim 1; or

that any terminal that runs the software described therein includes circuitry coupled and configured to compare during an authentication procedure (a procedure performed by a transmitter and a receiver by which the transmitter verifies that the receiver is authorized to receive protected content from the transmitter or the receiver verifies that the transmitter is authorized to send protected content to the receiver) distinctive values (e.g., serial numbers) allocated to the terminal and to another terminal and prevent authentication from succeeding if the distinctive values are equal, as does the device recited in amended claim 1.

There is no teaching or suggestion determinable from Anbinder that terminals should implement a content protection protocol in which one sends encrypted data to the other only after the terminals successfully complete an authentication procedure, or that a failed attempt by a terminal to complete an authentication procedure with a second terminal prevents the terminal from sending encrypted data to the second terminal. To the extent that Anbinder's teaching that a first terminal (that has commenced to run of a software copy having a serial number) should check whether a software copy having the same serial number is running on a second terminal amounts to a teaching that the first terminal should perform a content protection procedure, Anbinder teaches merely that determination by the first terminal during the procedure that the second terminal is running a software copy having a duplicate serial number should trigger notification of some unspecified entity ("you") that the second terminal is running a copy having a duplicate serial number. This does not amount to a teaching or suggestion that the determination by the first terminal (that the second terminal is running a software copy having a duplicate serial number) is or causes a failed attempt to complete an "authentication" that prevents the first terminal from sending encrypted data to the second terminal.

Anbinder also fails to teach or suggest a device for use in a system that implements a protocol, of the type recited in claim 2, requiring that a transmitter send a first distinctive value to a receiver and the receiver send a second distinctive value to the transmitter during an authentication procedure. Anbinder includes no teaching or suggestion that each terminal of any pair of terminals mentioned therein should send a serial number (or other distinctive value) to the other terminal of the pair during an authentication procedure.

Amended claim 3 recites a transmitter for use in a system configured to implement a content protection protocol which requires that each of a receiver (connected to the transmitter by a serial communication link) and the transmitter has a distinctive value allocated thereto, that the transmitter must send a first distinctive value (allocated to the transmitter) to the receiver and the receiver must send a second distinctive value (allocated to the receiver) to the transmitter during an authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the

transmitter sends encrypted data to the receiver. Amended claim 3 recites that the transmitter includes circuitry configured to compare a value (received over the serial communication link at an input of the transmitter) and the first distinctive value, to prevent authentication from succeeding if the compared values are equal, and to send encrypted data to the receiver over the link upon successful completion of the authentication procedure when coupled to the link. Anbinder fails to teach or suggest a transmitter having the noted limitations of amended claim 3.

Amended claim 4 recites a receiver for use in a system configured to implement a content protection protocol which requires that each of a transmitter (connected to the receiver by a serial communication link) and the receiver has a distinctive value allocated thereto, that the transmitter must send a first distinctive value (allocated to the transmitter) to the receiver and the receiver must send a second distinctive value (allocated to the receiver) to the transmitter during an authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the transmitter sends encrypted data to the receiver. Amended claim 4 recites that the receiver includes circuitry configured to compare a value (received over the serial communication link at an input of the receiver) and the second distinctive value, and to prevent authentication from succeeding if the compared values are equal. Anbinder fails to teach or suggest a receiver having the noted limitations of amended claim 4.

Amended claim 5 recites a system including a transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and receiver are configured to implement a content protection protocol which requires that the transmitter must send a first distinctive value to the receiver and the receiver must send a second distinctive value to the transmitter during an authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the transmitter sends encrypted data to the receiver. The transmitter includes circuitry configured to compare a value (received during the authentication procedure) and the first distinctive value, and to prevent authentication from succeeding if the compared values are equal. The receiver includes circuitry configured to compare a value (received during the authentication procedure) and the second distinctive value, and to prevent authentication from

succeeding if the compared values are equal. Anbinder fails to teach or suggest a system including both a receiver having the noted limitations of amended claim 5 and a transmitter having the noted limitations of amended claim 5.

Amended claim 28 recites a receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol that requires that the transmitter send a first distinctive value to the receiver during an authentication procedure, that the receiver send a second distinctive value to the transmitter during the authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the transmitter sends encrypted data to the receiver. The receiver includes circuitry configured to check whether the first distinctive value that it receives during the authorization procedure satisfies at least one predetermined criterion, and to prevent authorization from succeeding if said first distinctive value does not satisfy each said criterion. Anbinder fails to teach or suggest a receiver having the noted limitations of amended claim 28.

Amended claim 29 recites a transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol that requires that the transmitter send a first distinctive value to the receiver during an authentication procedure, that the receiver send a second distinctive value to the transmitter during the authentication procedure, and that the transmitter and the receiver must successfully complete the authentication procedure before the transmitter sends encrypted data to the receiver. The transmitter includes circuitry configured to check whether the second distinctive value that it receives during the authorization procedure satisfies at least one predetermined criterion, to prevent authorization from succeeding if said second distinctive value does not satisfy each said criterion and to send encrypted data to the receiver over the link upon successful completion of the authentication procedure when coupled to the link. Anbinder fails to teach or suggest a transmitter having the noted limitations of amended claim 29.

Claims 30 and 31 stand rejected under 35 U.S.C. 103(a) as being obvious over Anbinder. In response, Applicant respectfully contends that these claims are patentable over Anbinder for the following reasons.

Claim 30 recites a receiver including a lockout means configured to prevent successful completion of an authentication exchange between the receiver and a transmitter in the event that an authorization request is received at the receiver within a predetermined time window after a predetermined number of authentication requests have been received at the receiver. Anbinder fails to teach or suggest a receiver having such a lockout means, and the Examiner has not identified any such teaching or suggestion determinable from Anbinder.

Claim 31 recites a transmitter including a lockout means configured to prevent successful completion of an authentication exchange between a receiver and the transmitter in the event that an authorization request is received at the transmitter within a predetermined time window after a predetermined number of authentication requests have been received at the transmitter. Anbinder fails to teach or suggest a transmitter having such a lockout means, and the Examiner has not identified any such teaching or suggestion determinable from Anbinder.

Reconsideration and allowance of the claims, as amended, is respectfully requested.

Respectfully submitted,

GIRARD & EQUITZ LLP

Dated: 12/5/05 By: _____

Alfred A. Equitz
Reg. No.30,922

Attorneys for Applicant

Attorney Docket No. SII-600 (SIMG-0096)